

## Trustworthy Cyber-Physical Systems, Integrated Systems, and Networked Software

This paper presents some of the key areas of our interest that are desired networking and information technology (NIT) capabilities for critical aviation infrastructures as well as US defense and intelligence.

### Desired Future NIT Capabilities and Strategic Goals:

Air transportation around the world is evolving to overcome major challenges such as limited capacity, increased air traffic, and environmental pollution. Within the next two decades, advanced NIT enabled applications and processes will be introduced for enhanced aircraft operation, control and maintenance. Consequently, the next-generation airplanes and air traffic management are modeled as safety- and security-critical *cyber-physical systems* on which human lives and well-being depend. The emerging wireless, ad hoc, and sensor networks for aviation, US Air Force, and border control are also cyber-physical systems that are trusted to provide information that can be used in real-time, reliable, safe and useful decisions. Furthermore, recent NIT developments in aviation include *integration of systems* across diverse domains to facilitate network applications, and *open source software* based solutions for reduced manufacturing and maintenance costs of networked systems.

Therefore, to ensure safety, security, reliability, efficiency, usability and yield of future air transportation as well as battlefields, the strategic goal is to support, progress fundamental research and collaboration in the trustworthy design, development, verification and validation of cyber-physical systems, integrated systems, as well as networked software.

### Key Challenges and Research Priorities:

The following will require coordination between two or more agencies in the NITRD.

- Framework to formalize the relationship between security and safety.
  - Integration of the mainly discrete methods of security analysis into the quantitative, probabilistic approaches of safety analysis.
  - Combining security analysis which refers to non-functional properties, with the functional software correctness analysis to achieve an overall system safety level.
- Assessment of security technologies in the context of safety certification.
  - Evaluation of avionics software/systems for encryption and authentication.
- Long-term security mechanisms for airplane information assets.
  - Protection of information assets throughout airplane lifecycle.
- Effective formal methods.
  - Visual representations of FM with transparent analysis to facilitate the communication of FM benefits to business management.
  - Specification language that is accessible to software architects/developers without substantial training, and easy for customers to understand so they can contribute to the formal specification.
- High assurance of networked system-of-systems.
  - Interoperable domain standards and policies for NIT and security.
  - Design of scalable pervasive public key infrastructure for establishing trust in large-scale, multi-stakeholder aviation applications such as airplane software distribution.
  - Inexpensive, efficient, scalable, user-friendly methodologies for end-to-end assurance assessment.
  - Security models for multi-disciplinary global collaboration.
- Security of integrated modular systems

- Evaluation of potential impact of loadable software at different safety levels residing on the same platform
- Security assessment tools for cyber-physical systems.
  - Evaluation of trustworthiness of information received from the physical world.
  - Evaluation of the impact of attacks on the security and performance of networks.
- Evaluation of potential attacks on next-generation networked aviation
  - Security assessment of communications, navigation and surveillance technologies, such as Asynchronous Dependent Surveillance, before use for US air traffic management.
  - Securing operation and control of unmanned aerial systems for civilian applications
  - Secure design of onboard wireless networked control systems
- Early demonstration or evaluation of emergent security technologies.
  - Quantum cryptography.
- Human-computer interaction for airplane operators.
  - Introduction of onboard networks and security technologies will warrant data representation and network monitoring tools to ease the cognitive load of pilots, aircraft maintenance and traffic control personnel. Due to the safety-critical aspects of such software-based tools and the global operation of airlines, high confidence design and assessment is needed.
- Wireless-enabled environmental monitoring and control.
  - Wireless sensors deployed on the aircraft can provide feedback on pollution-related factors of legacy, current and future airplanes. However, key enablers for this include the design of efficient and non-interfering wireless sensor network architecture and the mitigation of security concerns.
- Trustworthiness and privacy of ubiquitous computing in aviation.
  - Addressing the lack of centralized authorities.
  - Assessment of user privacy concerns, such as traceability of RFID systems.
- Security of open source software.
  - Effective assessment methodologies for real-world open source software practices.
  - Metrics for determining assurance levels of open source products.

#### **Opportunities:**

- Common solutions for commercial and defense platforms. This approach has many benefits:
  - competitive advantages for airframe manufacturers from technology reuse.
  - employment of foreign nationals in the US for developing commercial platforms, derivatives of which are then offered to the US military.
- Common solutions for cyber-physical systems in aviation and other transportation sectors.
  - Recent advances in vehicular networks can benefit the aviation industry with the networking and security of e-enabled airplanes.

#### **Achieving Desired NIT Capabilities:**

NITRD should continue to support forums that allows industries to be forward looking in terms of identifying important technology areas, needs and challenges, and collaborate with universities to bring focused research and expertise in these areas. However, in aviation, diverse organizations have diverse interests and spans of control, sometimes overlapping and sometimes mutually contradictory. Therefore, the desired end-state must be a coherent set of regulatory laws, practices, processes that work together to satisfy needs of the public weal, requirements for compliance, and business interests of manufacturers, maintainers, and operators of transportation infrastructure and products.